RiskBased
SECURITY

2019 Year End Report

Vulnerability QuickView

Welcome

In the lead up to this year-end report, in which we reflect on what we've observed and learned from a complete year of vulnerability data, our team has also been doing some soul-searching regarding the nature of vulnerabilities themselves. Unlike the data breach landscape, where the results have been severely worsening quarter-after-quarter, the 2019 vulnerability disclosure landscape has been relatively steady.

Yes, we all know that CVE continues to fall short of our expectations (and those of the security industry as a whole), and for those who want that data, this report will still contain that analysis. However, there are some serious issues out there that we feel don't get adequate attention. Although our dedicated readers know that managing vulnerabilities is essential in maintain an organization's security posture, the nuances of vulnerabilities and their effects may get lost in translation when presented to the mainstream media.

Why do vulnerabilities matter? What effects do they have and what does the data tell us? Why should we care? These are the questions we have been asking ourselves as we put together this report. Not only has 2019 seen changes within the vulnerability landscape, but we have seen an issue that will reach a pinnacle in 2020. Risk Based Security has been collecting specific data to show readers why you should care: the findings show how vulnerabilities might affect the democratic institutions we hold dear.

We hope that you enjoy the latest Vulnerability QuickView Report.

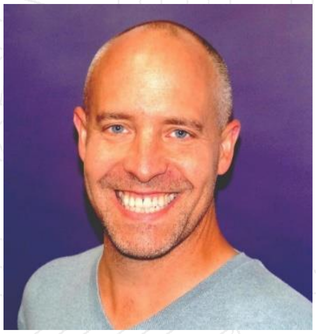
Sincerely,

RiskBased SECURITY

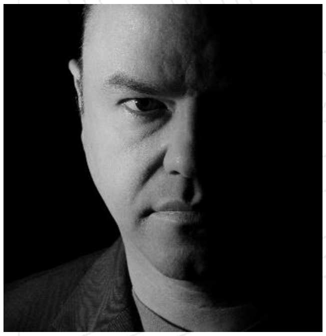
© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

In This Issue

FEATURING VIEWPOINTS FROM



Paul Garden
Senior Product Marketing Manager,
JFrog



Brian Martin
Vice President,
Vulnerability Intelligence,
Risk Based Security

WELCOME

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Key Highlights

- Risk Based Security's VulnDB team aggregated 22,316 newly-disclosed vulnerabilities during 2019.
    - 33.43% of all vulnerabilities identified in 2019 had a CVSSv2 score of 7.0 and above.
    - 37.26% of all vulnerabilities identified in 2019 had available exploit code or a Proof of Concept (PoC).
- Risk Based Security has identified 302 vulnerabilities in Electronic Voting Machines (EVM), 289 of which have no known solution.
    - Of the remaining 13, eight have available remediation steps, but only one has a CVE ID.
    - Vulnerable EVMs have been used in previous elections and they will most likely be used again in the upcoming 2020 elections.
- Patch Tuesday is getting out of hand, with an all-time high of 327 vulnerabilities being disclosed in a single day. This is a daunting number of vulnerabilities for organizations to deal with.
    - Adobe and Microsoft made up 62% of the vulnerabilities released on that day in 2019.
- Despite a low CVSSv2 score, the RIDL / ZOMBIELOAD vulnerability, continues to run rampant affecting over 450 products, and still growing.
    - This vulnerability has been observed being used in the wild by at least three different Chinese hacking groups: Iron Tiger, APT3, and Calypso.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Seven Steps to Achieve DevSecOps and SCA Nirvana in 2020

Paul Garden, Senior Product Marketing Manager, JFrog

Paul heads up the DevSecOps Product Marketing function at JFrog, and has a passion for sharing open source software best practices for the developer and security engineer community. Originally a native of the UK, Paul now makes his home in the San Francisco Bay area. When he's not busy helping you keep your software safe and secure; you can find him playing golf or wine tasting in the Santa Cruz Mountains.

2019 was a growth year for the world of DevSecOps, with more companies embracing security as an integral part of their growing DevOps pipelines. The number of DevSecOps tools and frameworks choices is vast and can be confusing for IT and DevOps professionals, often leaving them with tool fatigue as they try to understand and integrate multiple solutions into their software development pipeline as well as their Software Composition Analysis (SCA).

But why is this becoming such a focus in the first place? To keep up with the pace of innovation, open source software usage has exploded, and is now commonplace in application development pipelines. As more and more source code come from the "outside," the need to corral and understand its contents is now mission-critical. As we head with excitement into 2020, we'll take a look at the types of tools and technologies that should be most successful in mitigating vulnerabilities that are possibly contained in open source software (OSS).

MODERN DEVELOPMENT REALITIES

With the growth in open source adoption, Industry wide sentiment is that the typical application may now be composed of over 50% OSS components. This trend is driving up the number of exploits seen, because of the publicly-available open source libraries. Companies are reacting by adding more security checks, integrated into their DevOps pipelines.

But what types of tools do security pros and developers really need to ensure the safety and stability of their production software? In fairness, there are a few different broad categories of DevOps security tools that address different areas of the Software Development LifeCyle (SDLC):

- Code Analysis (Static & Dynamic)
- Software Composition Analysis (3rd party OSS)
- Run-time Security Analysis (including Containers)

Ideally teams should aim to adopt all of these areas for complete SDLC security, but for this brief article, we'll focus on Software Composition Analysis, which specifically targets mitigation of vulnerabilities and license compliance violations in OSS components and binaries.

Here are 7 things you need to ensure as you select DevSecOps tools in 2020:

1. DEMAND TOOLS THAT CAN MANAGE AND UNDERSTAND ALL ARTIFACTS NATIVELY

Before teams even get to the task of identifying which OSS components have vulnerabilities, they first need a universal DevOps platform that can (as a basic requirement) manage all artifacts and binaries in a central place, regardless of their type and technology. It needs to know which artifacts are used, consumed or created and what their dependencies are.

2. GRAB THE BEST FUEL

The most effective solutions will require the power of a world class vulnerability intelligence solution like VulnDB, to make sure it has the most up-to-date vulnerability knowledge. The best cars in the world are nothing if they don't have great fuel to propel them.

3. INSIST ON VISIBILITY AND IMPACT ANALYSIS

The DevSecOps "winners" in 2020 will not only be able to understand which OSS libraries and components your binaries use, but also how to unpack and scan them to see into all of the underlying layers and dependencies - even those packaged in Docker images and zip files. A solution that can understand an organization's artifact and dependency structure, can provide visibility and determine the impact of any vulnerability or license violation discovered anywhere in a software ecosystem.

4. ABSOLUTE GOVERNANCE

Table stakes in this space are the ability to automate Governance in cooperation with a company's security office. A governing system will need to be able to automatically enforce company policies, and be able to take action accordingly without intervention:

- Notification of security or compliance violations
    - Email, Instant Messages, Jira, etc.
- Blocking of downloads
- Failing of builds that depend on vulnerable components
- Prevention of the deployment of vulnerable release bundles

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

5. GO BROAD ACROSS THE PIPELINE

Differentiators in 2020 will be solutions that know how to take this exhaustive data and connect it to the security scans of all the binaries across repos, builds and containers. A platform that can stretch across the whole SDLC and continuously detect/monitor for vulnerabilities and compliance violations, even after production deployment, will stand out from the crowd.

6. GO HYBRID

Even if you're not maintaining a hybrid infrastructure yet, you will. Selecting tools and solutions now that support your ongoing cloud journeys and hybridization of your infrastructure will ensure you have consistency and standards across your DevSecOps pipelines wherever they may live.

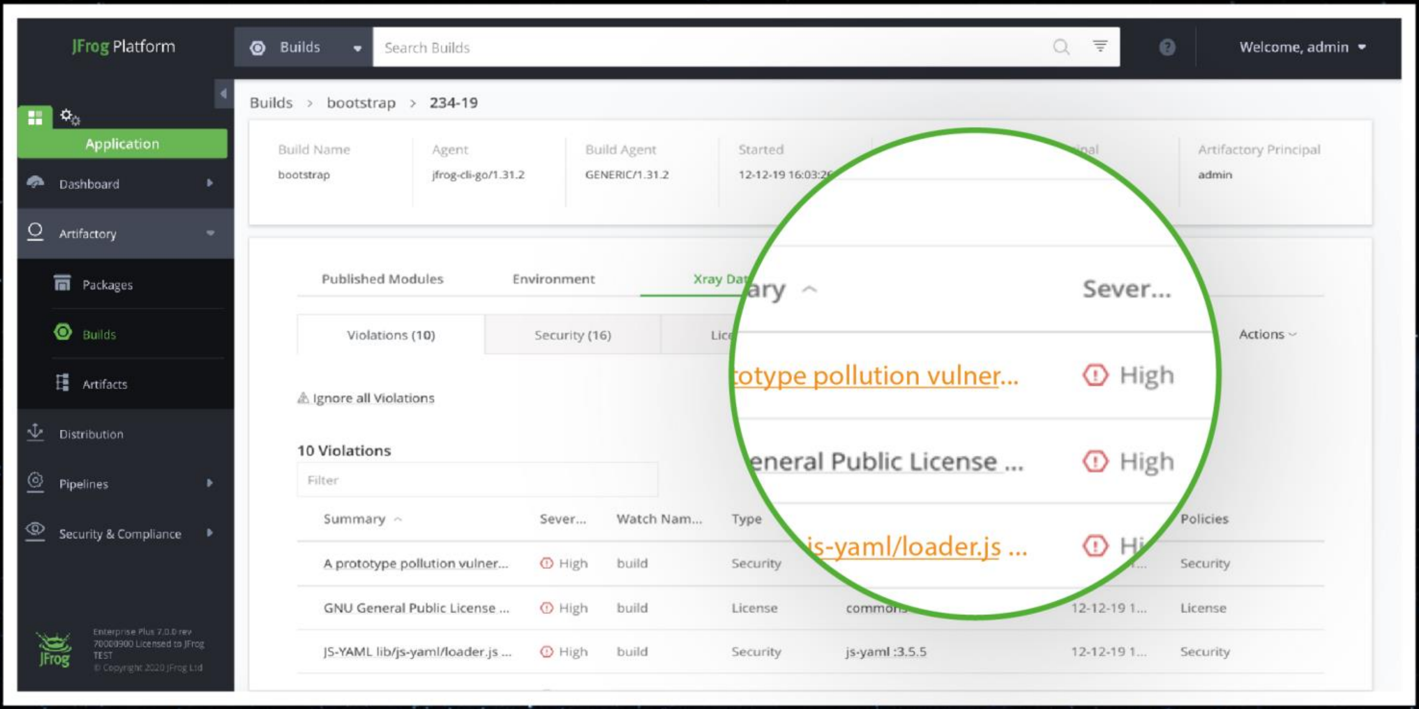
7. BONUS: EDUCATE EVERYONE

DevSecOps is no longer a wish list item for a CIO, it is now a must-do IT strategy which needs to be an integral part of any software development lifecycle. Even when an organization has chosen a DevSecOps winner, leaders need to make sure that they implement a sound DevSecOps process across teams. This includes the need to continually educate developers and DevOps practitioners on application security best practices. Developers outnumber security professionals by 100:1 and this ensures distributed security knowledge across development teams, essential to closing the vulnerabilities gap faster.

CLOSING THOUGHT

Choosing a DevSecOps platform that can manage repositories, binaries, CI/CD automation, OSS component analysis, and supports containerized release frameworks can seem a daunting task. Further, supporting your On-prem, Cloud, Multi-Cloud and Hybrid deployments is an additional complication. But starting with a checklist of what to demand in a solution is a great place to start.

THE BEST UNIVERSAL DEVSECOPS PLATFORM...



Builds > bootstrap > 234-19

Build Name	Agent	Build Agent	Started		Artifactory Principal
bootstrap	jfrog-cli-go/1.31.2	GENERIC/1.31.2	12-12-19 16:03:2		admin

10 Violations

Summary	Sever...	Watch Nam...	Type			Policies
A prototype pollution vulner...	High	build	Security			Security
GNU General Public License ...	High	build	License	common	12-12-19 1...	License
JS-YAML lib/js-yaml/loader.js ...	High	build	Security	js-yaml :3.5.5	12-12-19 1...	Security

...REQUIRES THE BEST INTELLIGENCE

JFrog + VulnDB

TRY IT TODAY AT:

JFROG.COM/XRAY/FREE-TRIAL

Electronic Voting Machines; That Old Redux…

Brian Martin, Vice President of Vulnerability Intelligence, Risk Based Security

Brian has been studying, collecting, and cataloging vulnerabilities for twenty-five years both personally and professionally. He has pushed for the evolution of Vulnerability Databases for years via blogs, presentations, and public dialogue on social media, and has helped change them to improve their processes and coverage. He was previously a member of the CVE Editorial Board for ten years and continues to rigorously follow the changing landscape of the vulnerability database ecosystem.

> *"With no doubt, electronic voting machines with vulnerabilities have been used in past elections and will be used again the next election."*
>
> Brian Martin, Vice President of Vulnerability Intelligence, Risk Based Security

Integrity is one of the cornerstones to both the concept and the practice of Information Security. We want to make sure that the integrity of the systems we use remains intact. It doesn't matter if it is your smart watch, smart IoT device, laptop, workstation, automobile, or an airplane. If it has a connection, bad people can do bad things to those systems, and the consequences can range from annoying to deadly.

Overall, the word "integrity" has been a hot topic in 2019 and it will continue to dominate most of 2020. You can't go more than a few minutes on social media without seeing something about politics, and more specifically, the next election. Whether it is the next county or presidential election, those elections are increasingly performed using "electronic voting machines" (EVMs) to tally the votes. As with any device that relies on code, there are vulnerabilities that can affect the system's integrity, and you don't want someone tampering with them. It doesn't matter what politics or beliefs you subscribe to; the essence of democracy is that an election captures the will of the people.

A SEVERE LACK OF ATTENTION

Even though EVMs are instrumental in the democratic process, EVM security has received very little attention outside of InfoSec journalism. One of the most prominent journalists covering election security is Kim Zetter, who does a phenomenal job. Other than Zetter and Matt Bishop, an academic who has lead teams that discovered EVM vulnerabilities and challenges the status quo, the only security researchers that seem to '*sound the alarm*' have been Risk Based Security (RBS). Even before joining the RBS team as a Principal, I took a specific interest in EVM security throughout 2009 in the context of formally cataloging their known vulnerabilities. While there were several academic papers that went into amazing detail in determining the flaws, they were lost to the general public because they are so complex and challenging to communicate. To me, this was a combination of the way academics approached vulnerability research, along with the ways EVMs fundamentally differ from other computers, such as their interfaces and singular purpose.

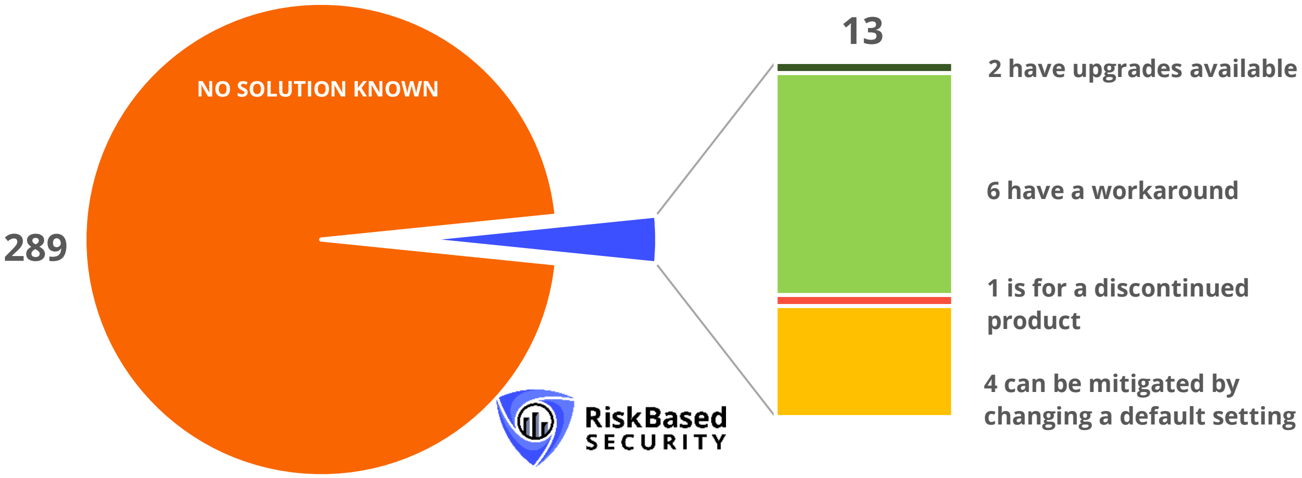
Despite the lack of attention, I was trying to highlight the potential impact of these vulnerabilities in 2012 saying, "*Prepare to be scared for the coming elections*." Jump to 2016 and RBS was describing the situation as "*an Old but Looming Threat*" with 260 EVM vulnerabilities. In 2018, we again talked about the threat (now no longer "looming", as concerns of foreign meddling saturated the news), with 292 EVM vulnerabilities documented. Hopefully we don't sound like a broken record given the time between posts, but if there is a topic in computer security worth talking about, it is this one.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

THE CURRENT STATE OF EVM SECURITY

As of this report, we stand at 302 documented vulnerabilities in Electronic Voting Machines and 96% of them do not have a solution available. To make matters worse, of those, only one vulnerability (0.3%) has a CVE ID assignment and is cataloged in the U.S. National Vulnerability Database. That's right, just **one**. Even if election precincts have security processes or audit standards, or conduct vulnerability scans, they are likely based on policies, methodologies and scanners that rely on CVE for vulnerability intelligence. This means that election precincts won't be aware of these issues because their security solutions won't even know that there is an issue to begin with. There is no doubt that electronic voting machines with vulnerabilities have been used in past elections, and will be used again in the next election.

There are **302** known vulnerabilities for Electronic Voting Machines.

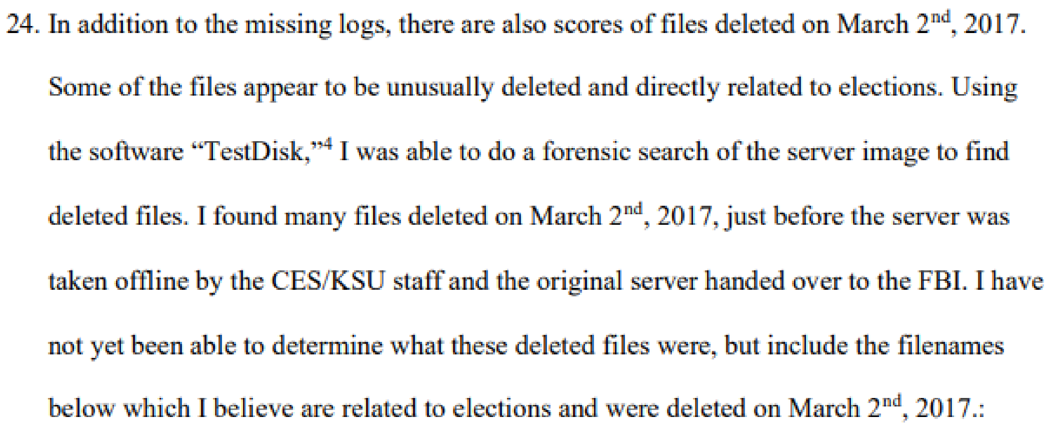


Currently, Election Systems & Software (ES&S) still sells their popular ExpressPoll tablet, which "*gives poll workers a simple-to-operate device that reduces check-in and verification waiting time for voters, increases the accuracy of ballots issued and improves the Election Day experience for all*." Unfortunately, there are nine vulnerabilities known in those devices, none of which have a solution. Can it get worse? Sadly, yes. These vulnerabilities include default, hard-coded administrator credentials, no encryption for polling information, and ways for a voter to subvert the entire machine to manipulate votes. This isn't a one-off case either. ES&S links to a blog touting that North Carolina certified their ExpressVote (which according to ES&S doesn't have any published vulnerabilities) and also touts that their iVotronic device "*currently serves more than 2.4 million voters*" in the state. But despite their claim, that device has seventeen published vulnerabilities.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

THE EVIDENCE IS DAMNING

Regarding the EVMs, some skeptics say "*that the system is accurate and safe for continued use*". This and other statements repeatedly tout the security, saying that experts test the systems every election. However, when one expert was called to examine a machine, that isn't what he found. Instead, he presented damning evidence in a finding that suggested systems were tampered with, or potentially compromised fully. Even more concerning is that the system in question was tampered with again just before it was handed over to the FBI during an investigation.



24. In addition to the missing logs, there are also scores of files deleted on March 2nd, 2017. Some of the files appear to be unusually deleted and directly related to elections. Using the software "TestDisk,"[4] I was able to do a forensic search of the server image to find deleted files. I found many files deleted on March 2nd, 2017, just before the server was taken offline by the CES/KSU staff and the original server handed over to the FBI. I have not yet been able to determine what these deleted files were, but include the filenames below which I believe are related to elections and were deleted on March 2nd, 2017.:

INTEGRITY

In 1818, Benjamin Franklin wrote in his memoirs the following quote which speaks to the cornerstone of democracy and the importance of EVM security: "*...they who have no voice or vote in the electing of representatives, do not enjoy liberty, but are absolutely enslaved to those who have votes and their representatives.*"

Integrity. It is a cornerstone of Information Security. One thing we're sure of is that electronic voting machines, regardless of vendor, do not demonstrate that integrity is part of their design and implementation. They have hundreds of vulnerabilities, their systems are designed so there are little to no audit trails, and there are too many past cases of systems being tampered with. This should be of deep concern to every American.

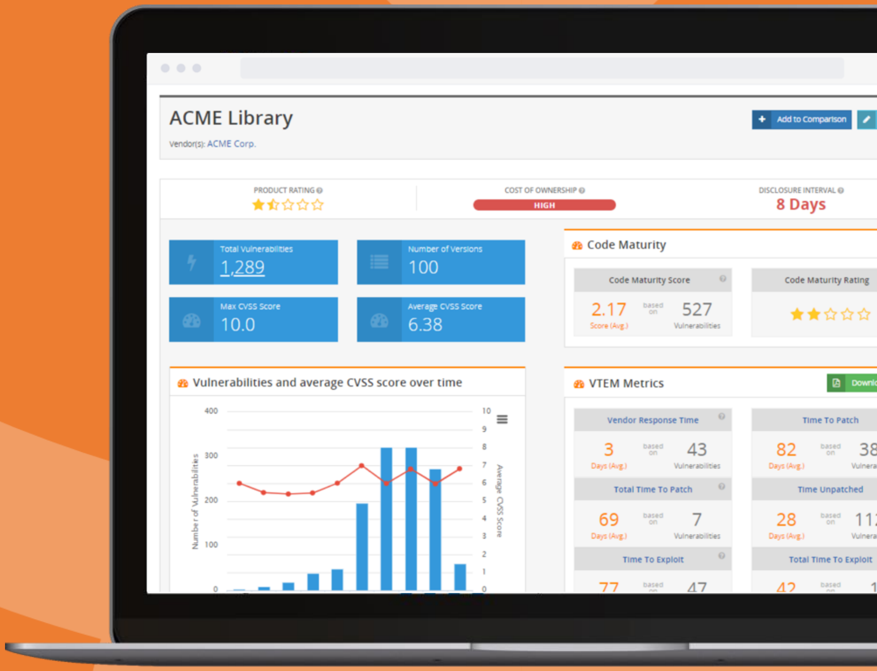
© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

The Vulnerability QuickView report is powered by

VulnDB

The most comprehensive, detailed and timely source of vulnerability intelligence and third-party library monitoring.

- ☑ DevSecOps
- ☑ Security & Vulnerability Management
- ☑ Vendor Risk Management
- ☑ Procurement
- ☑ Governance & Management



ACME Library

Vendor(s): ACME Corp.

PRODUCT RATING ★⯪☆☆☆

COST OF OWNERSHIP HIGH

DISCLOSURE INTERVAL 8 Days

Total Vulnerabilities 1,289

Number of Versions 100

Max CVSS Score 10.0

Average CVSS Score 6.38

Code Maturity

Code Maturity Score 2.17 Score (Avg.) based on 527 Vulnerabilities

Code Maturity Rating ★★☆☆☆

Vulnerabilities and average CVSS score over time

VTEM Metrics

Vendor Response Time 3 Days (Avg.) based on 43 Vulnerabilities

Time To Patch 82 Days (Avg.) based on 38 Vulnera

Total Time To Patch 69 Days (Avg.) based on 7 Vulnerabilities

Time Unpatched 28 Days (Avg.) based on 11 Vulnera

Time To Exploit 77 based on 47

Total Time To Exploit 42 based on 1

REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE
vulndb.cyberriskanalytics.com

Vulnerability Trends of 2019

2019 At A Glance

Overall, the vulnerability disclosure landscape in 2019 can be summed up in a phrase: “Business as Usual”. Avid readers of this report may recognize that the figures below are eerily similar to those of 2018. Interestingly enough, we are seeing the same trends as last year, just like clockwork.

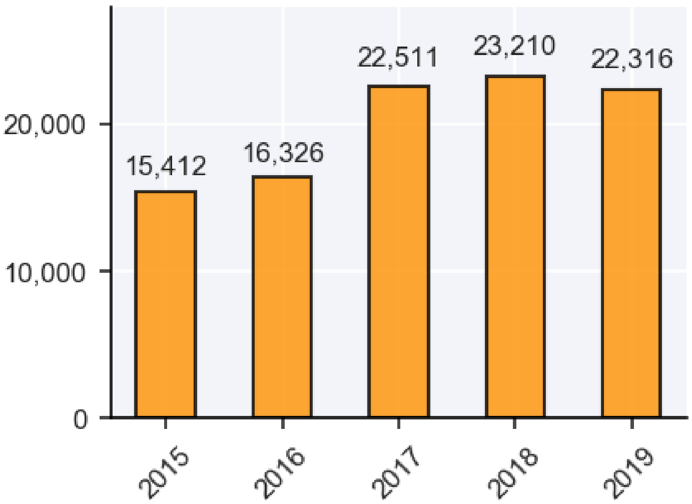


Figure 1: Number of vulnerabilities disclosed in the last five years

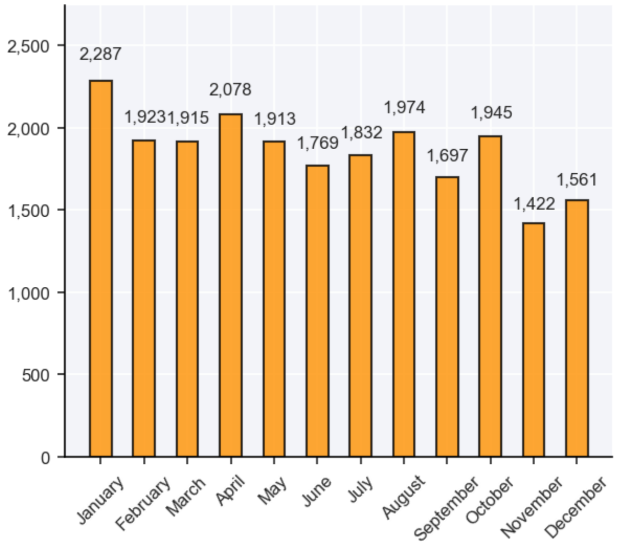


Figure 2: Number of vulnerabilities disclosed each month in 2019

Consider that when our 2018 year-end report was published in February 2019, we reported that 22,022 vulnerabilities had been disclosed in 2018. If we compare that number against our current tally for 2018 (23,210), over a thousand vulnerabilities were identified after the publication of our report and we expect more to come. Our standard practice is, as always, to collect the best and more accurate vulnerability intelligence available, and this includes revisiting prior years to pick up any “new” vulnerability disclosures as we continue to expand our source coverage.

As we’ve mentioned in previous years, this can make the narrative murky at times. If you compare our fresh-off-the-press number for 2019 to our most current tally from 2018, there was a 3.9% decrease in vulnerabilities between this year and last. If you consider the best numbers available at the time of the report being published, there was actually a slight (1.3%) increase. With this disclaimer, you can see how it’s hard to determine whether vulnerability disclosures are really getting more or less frequent. We can certainly agree that the quality of software is not getting significantly better.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Critical (Library) Vulnerabilities Missing from CVE

As we have demonstrated over the years, CVE continues to fall short in aggregating vulnerabilities. A more important aspect of this becomes, "*what did they miss?*" By the end of 2019, 674 vulnerabilities disclosed last year with a CVE ID are still in RESERVED status, meaning the ID is assigned by the entry in their database is not public. However, any notion that the missed vulnerabilities are in software you will never see in a production network are immediately dismissed. The vulnerabilities with a 'critical' score (CVSS 9.0 - 10.0) in high-use third-party libraries alone should be of great concern. Consider FFmpeg, forked over 6,000 times on GitHub, or OpenSSL, forked over 5,000 times, libraries that provide critical functionality to tens of thousands of software packages, have critical vulnerabilities without a CVE. Other libraries such as Google V8 and WebKit, the latter of which can be found in Safari, BlackBerry browser, Tizen, and more. Components of WebKit can also be found in Google Chrome and Opera.

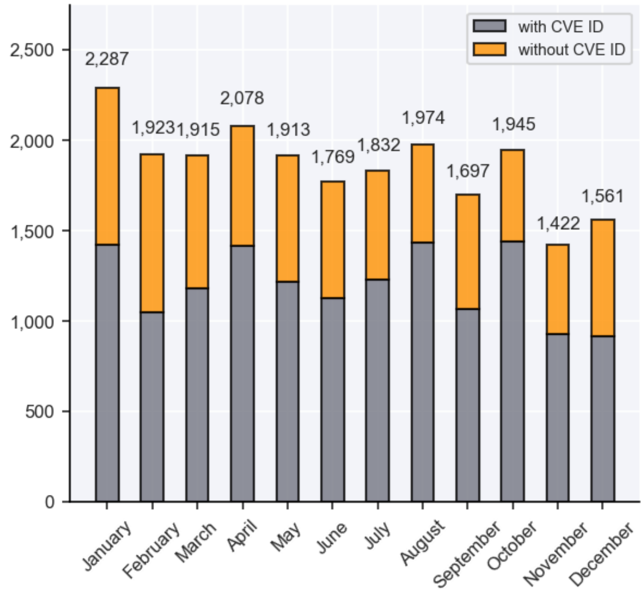


Figure 3: Number of vulnerabilities disclosed in 2019, with and without CVE IDs

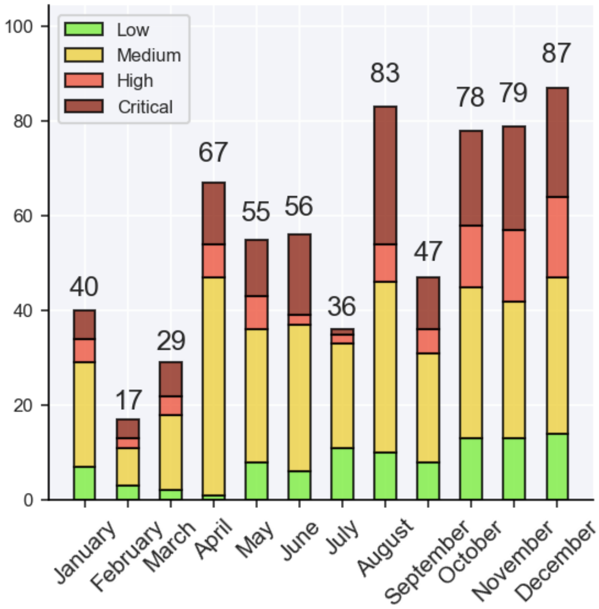


Figure 4: Number of vulnerabilities disclosed in 2019 in RESERVED status, with severity

History has shown us that major parts of our life, both personal and professional, have moved to web-based platforms. From browser to web server, the data we see and share will be passed through and processed by dozens of third-party components, sometimes hundreds. Organizations may assume that third-party components have been analyzed for vulnerabilities and are safe to use in commercial products, but unfortunately, that often isn't the case. Overall, decision makers need to be aware that they may be inheriting security issues when these third-party components are incorporated, and that these issues most likely will be missing from CVE.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

"Top" Vendors by Confirmed Vulnerabilities

Now that we've reached the end of the year, we can take a look at the scoreboard for most disclosed vulnerabilities in 2019. Compared to 2018, the composition of the top 10 is relatively the same, with the exception of Cisco rising up into the top 10 and replacing Samsung. The single biggest change between 2019 and the previous year is Oracle disclosing 600 fewer vulnerabilities. As we've mentioned previously, that gap is actually much smaller as we will be identifying more vulnerabilities disclosed in 2019 as time goes on, particularly in major vendors like Oracle.

Vendors	New Rank	Old Rank	2019 Totals	2018 Totals
SUSE	1	1	1379	1689
Software in the Public Interest, Inc.	2 ⬆	4	1264	1312
Oracle Corporation	3 ⬇	2	1064	1677
IBM Corporation	4 ⬆	5	1054	1311
Google	5 ⬇	3	1046	1609
Canonical Ltd.	6 ⬆	7	978	1158
Microsoft Corporation	7 ⬆	9	926	804
Red Hat, Inc.	8 ⬇	6	911	1259
Dell	9 ⬇	8	701	859
Cisco Systems	10 ⬆	10+	615	532

Table 1: Top ten vendors by vulnerability disclosures in 2019, as compared to 2018.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Disclosures Over Time & Patch Tuesday

October 2003 brought us the phenomenon "Patch Tuesday". Created by Microsoft, it gave us the same 'day' each month that they would release security patches. The second Tuesday of each month would become a single day in which organizations could expect the disclosures, and roll out the patches in a more scheduled and consistent manner. What started with Microsoft turned into several other companies that began piggybacking their releases on that day including Adobe, SAP, Siemens, and Schneider Electric. To make it better/worse for some organizations, more companies found themselves releasing on Patch Tuesday at times, but not consistently. They include Google, Apple, Mozilla, Intel, Cisco, F5, and Juniper. All of those potential releases are in addition to the typical disclosures seen on any given day.

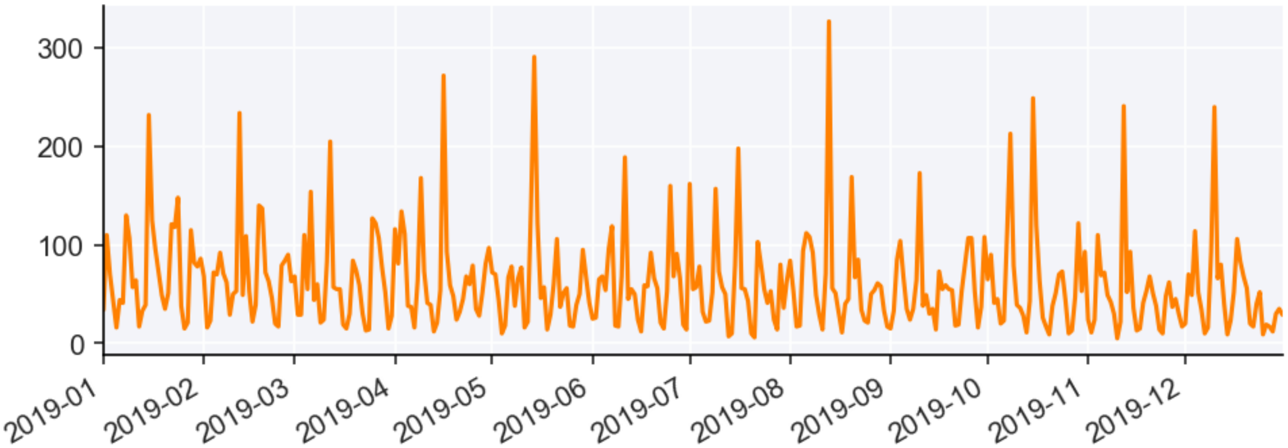


Figure 5: Number of disclosures each day in 2019

Visually, this looks interesting! Almost every month shown in the chart above have a distinct spike that corresponds with Patch Tuesday. One in particular rises above the others, August 13, 2019 which saw 327 disclosures that day. That day saw disclosures from many of the usual suspects, but 62% came from Adobe (114) and Microsoft (88). That day also saw eight vulnerabilities disclosed in Hypertext Transfer Protocol Version 2 (HTTP/2) that didn't come with a name, logo, or web site. This illustrates how Microsoft's intentions over fifteen years ago have been co-opted, and turned that one day into a nightmare for many organizations. Coordinated Disclosure is all the rage when researchers find vulnerabilities. Perhaps a better coordinated "Patch Tuesday" could benefit the organizations impacted by the vulnerabilities being released.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Exploit & Solution Trends

Evolution of Exploits Over Time

In what may be slightly good news for blue teams, while the number of vulnerabilities published with exploits over the last five years has grown, that increase is marginal. More importantly, the number of vulnerabilities published with no working proof-of-concept (PoC) or functional exploit has grown considerably, almost doubling in the same period. This may offer a small bit of relief for teams that monitor for threats and defend networks.

Why this change? There is no definitive reason why this increase in 'exploit unknown' happened. There are several factors that likely contribute to this. The first is an increase in fuzzing-related disclosures that produce crash information and other technical details proving a flaw is there, but the actual crashing input not being included. A second reason may be cataloging more disclosures from vendors that often provide vague details of the fixed issue and no exploit code. A third aspect that may be at play is an increase in a given type of disclosure that historically does not come with a fully functional exploit, such as SQL injection or XXE issues.

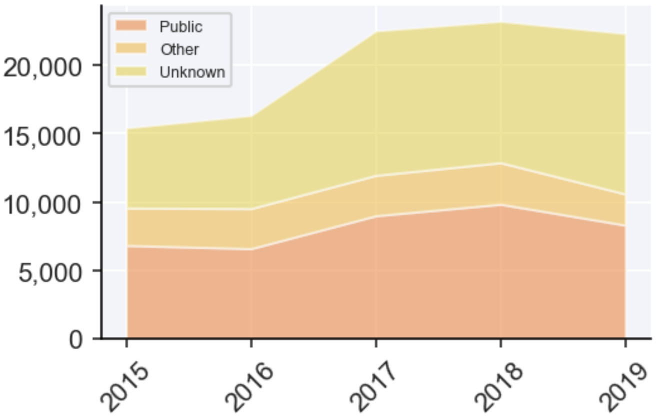


Figure 6: Evolution of exploit availability over time, 2019

Evolution of Solutions Over Time

Our reports show that the vulnerability landscape is not "getting better". We know that vulnerabilities will continue to be disclosed moving forward, and that the yearly totals are very likely to continue to rise over time. A more apt question to ask, instead of "*are things getting better*", might be "*are solutions getting better?*"

While we typically show the number of vulnerabilities with different types of solutions, such as patches or upgrades, this chart gives a better representation of how we're seeing more vulnerabilities with solutions each year. Over the last five years, we have seen a really interesting increase in both "solution unknown" along with some form of solution.

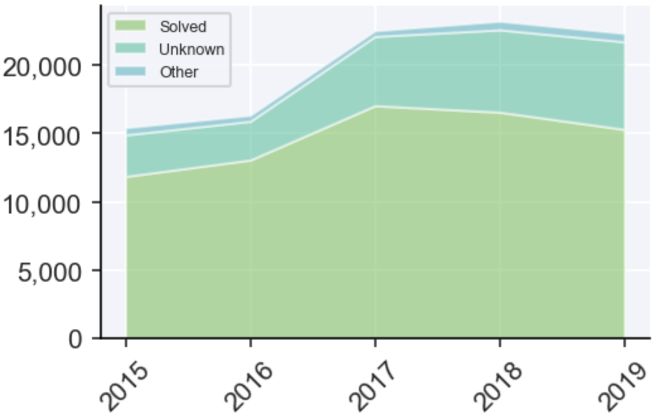


Figure 7: Evolution of solution availability over time, 2019

It is important to note that while a vulnerability may have a solution, it may be in the form of a commit made against the development branch of a project. Most companies will not do one-off patches by integration into their own code base, instead, favoring a formal release of the project from the vendor.

However, what happens when a vendor doesn't release a new version for over two years? These are some of the questions that may haunt security teams and lead to a lot more work in the form of code-level patches.

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

2019 Vulnerability Highlight

RIDL / ZOMBIELOAD

Intel Multiple Processors Speculative Execution Functionality Microarchitectural Fill Buffer Data Sampling (MFBDS) Local Kernel Information Disclosure (RIDL-L1DES / ZombieLoad)

That is certainly a solid mash-up of technical terms that isn't easy to digest. What is it? Known as "ZombieLoad", it is one of many variants of speculative execution vulnerabilities in Intel processors that allow a local attacker to gain access to privileged bits of information stored in the computer's active memory. Such attacks enjoyed a renewed popularity in March 2018, with the release of one dubbed "BranchScope". Over a dozen more followed since. One of those disclosed was known as "RIDL", short for "*Rogue In-Flight Data Load*", and it was initially determined to represent four distinct vulnerabilities including the Fallout variant in a second paper. In a case of mutual discovery, another team discovered one of the same variants that the RIDL team did, thus our designation of RIDL / ZombieLoad in our title.

IMPORTANCE OF A LIVING DATABASE

While a lot of these attacks got fun names like Plundervolt, NetCat, and SPOILER, it turns out that ZombieLoad has received the most attention of sorts. It may not dominate the news headlines, but our entry for ZombieLoad contains the most references (286) and affected products (417) out of all vulnerabilities disclosed in 2019. Even in the two weeks of writing this report after we took a snapshot of the data, the number of affected products jumped to over 450 and is still growing. This entry is a perfect example of the concept of a "***living database***", something we take pride in. When we add a vulnerability, we don't just move on and consider it a page in the history book. We update hundreds of entries a day with additional information, as seen by the number of references and products in this entry.

There are several interesting aspects about ZombieLoad and other speculative execution attacks that interest us, and keep in mind a vast majority of disclosures are mundane to us. Perhaps the most striking is that while these attacks require local access and receive a CVSSv2 score of 2.1 (low risk), they tend to get named and a lot of media attention. Despite that low risk, ZombieLoad has been observed being used in the wild by at least three different Chinese hacking groups (Iron Tiger, APT3, Calypso).

In the fascinating evolution of Intel processor speculative execution attacks, which we'd love to see written, comes two of the variants: ZombieLoad on April 29th, along with a ZombieLoad v2 variant on November 12th (also known as RIDL-TAA). With all of the variants and public attention, it is interesting to note how exceedingly difficult they are to patch. When we update software, it is a serious annoyance if it breaks some functionality or introduces new annoying behavior. When a computer processor vendor issues a patch, the stakes are higher. Imagine installing a patch and your computer's processor just stops working, leaving your entire computer dead in the water. While Intel is carefully releasing patches for these issues, it has rapidly become a game of whack-a-mole as each new variant pops up. As Wired summarizes:

> "AFTER 18 MONTHS, INTEL IS STILL TRYING TO FIX A SECURITY FLAW IN ITS CHIPS KNOWN AS MDS OR "ZOMBIELOAD" – NOW WITH A THIRD PATCH TO COVER YET ANOTHER VARIANT OF THE ATTACK. RESEARCHERS POINT OUT THEY TOLD INTEL ABOUT THE SECOND & THIRD VARIANTS A YEAR AGO."
>
> Wired

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved

Methodology and Terms

VulnDB is derived from a proprietary methodology and daily analysis of thousands of vulnerability sources. Unlike some vulnerability database providers, Risk Based Security is constantly searching for and adding new sources, in addition to working closely with customers to ensure coverage of the products they use.

VulnDB counts only distinct vulnerabilities. Products sharing the same vulnerable codebase are considered only one unique vulnerability. We do not consider vulnerabilities that affect multiple products as unique vulnerabilities as some vulnerability databases do, which artificially inflates their numbers. To be clear, a vulnerability in a third-party library such as OpenSSL is treated as one vulnerability; the multiple projects using and integrating that code do not constitute additional unique vulnerabilities, and are not included in any VulnDB counts.

CVE: Mission vs. Expectations

One of the fundamental objectives of VulnDB is to expand our search methods and collect as many vulnerabilities as possible, to provide our clients with the most comprehensive vulnerability intelligence available, allowing them to determine which vulnerabilities are important to their organization.

While we maintain a curated list of thousands of sources that are monitored on an hourly, daily, and weekly basis, new sources are discovered and/or are brought to our attention every day. CVE on the other hand, issues CVE IDs when requested by a vendor or researcher. Their mission is not to search for vulnerabilities like a vulnerability intelligence company. Rather, they are charged with assigning IDs and keeping minimal records.

Why then do organizations, scanning companies, risk platforms, and security service providers continue to use CVE/NDV as a vulnerability intelligence service and continue to insist that it is “good enough”? Who is best served by this approach? Certainly not those organizations, government agencies and consumers victimized by the increasing number of data breaches from exploited software vulnerabilities.

About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Vulnerability Intelligence, Vendor Risk Ratings, and Data Breaches. Our products, Cyber Risk Analytics (CRA), VulnDB and YourCISO, provide organizations access to the most comprehensive threat intelligence knowledge bases available, including advanced search capabilities, access to raw data via API, and email alerting to assist organizations in taking the right actions in a timely manner.

For more information, visit www.riskbasedsecurity.com or call +1 855-RBS-RISK.

About VulnDB

VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities via an easy-to-use SaaS Portal, or a RESTful API that allows easy integration into GRC tools and ticketing systems. VulnDB allows organizations to search and be alerted on the latest vulnerabilities, both in end-user software and the 3rd Party Libraries or dependencies

A subscription to VulnDB provides organizations with simple to understand ratings and metrics on their vendors and products, and how each contributes to the organization’s risk-profile and cost of ownership.

REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE
vulndb.cyberriskanalytics.com

NO WARRANTY

Risk Based Security, Inc. makes this report available on an “As-is” basis and offers no warranty as to its accuracy, completeness or that it includes all the latest data breaches. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based Security, Inc. for more detailed data loss analysis and security consulting services.

*”Zombie” icon from icons8.com

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved